

ROUTING AND RECORD SHEET

SUBJECT: (Optional)

Revision of DCIDs 1/7 and 1/20

FROM:

C/PPG/OS
4E-70, Hdqs.

EXTENSION

NO.

DATE

26 October 1982

STAT

STAT

TO: (Officer designation, room number, and building)

DATE

RECEIVED

FORWARDED

OFFICER'S INITIALS

COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)

1. C/Ops/PSI
4E-58, Hdqs.

Please review and forward comments/concurrence by 10 November 1982.

2. C/Ops/PTAS

27 OCT 1982

1027 HKE

3. C/SSC
5E-1, Hdqs.

4. C/SS/CL

5. C/SS/OTEE

6. C/Phy SD

28 OCT 1982

29 OCT 82 DB

7. DC/PSD

29 OCT 1982

8.

9.

10.

11.

12.

13.

14.

15.

Don't have your people take the look at the pl -

STAT

STAT

STAT

STAT

6-7: Pls handle yourself.

~~CONFIDENTIAL~~
DIRECTOR OF CENTRAL INTELLIGENCE


Security Committee

SECOM-D-346

21 October 1982

MEMORANDUM FOR: Members, DCI Security Committee

FROM:


Chairman

25X1

SUBJECT: Revision of DCIDs 1/7 and 1/20

Attached for your review and concurrence or comment is a memorandum to me from the Chairman of the SECOM Compartmentation Subcommittee forwarding draft revisions of DCIDs 1/7 and 1/20. I plan to ask for a formal vote by members on these revisions at the next meeting of the SECOM, scheduled for 17 November 1982.

25X1

Attachment



FOR OFFICIAL USE ONLY
When Attachment Removed

OS 2 2593/1

~~CONFIDENTIAL~~

HEADQUARTERS AIR FORCE INTELLIGENCE SERVICE
WASHINGTON DC 20330REPLY TO
ATTN OF:

INS

19 OCT 1982

SUBJECT: Revision of DCIDS (U)

TO: Chairman
DCI Security Committee

1. (U) Your memorandum (SECOM-D-326), 27 Sep 82, same subject, tasked the Compartmentation Subcommittee with reviewing and revising DCIDS 1/7 and 1/20 by 5 Nov 82.
2. (U) The Compartmentation Subcommittee has concluded its task and unanimously approved the attached draft revisions of the two DCIDS.

a. (U) DCID 1/7 Revision. Except as follows, the attached primarily reflects format and editorial revisions made necessary by recent NFIB policy on the restructuring of DCID directives and related policy statements.

(1) (U) The phrase "and related material" was added after the word "intelligence" in the last sentence of paragraph 6f. This change was suggested by the NSA member to broaden the application of the "REL _____" control marking.

(2) (U) Paragraph 4 was added to the Appendix at the request of the Air Force member to implement NFIC-30.1/6, 16 Aug 82, concerning policy on contractor operation of all-source telecommunications centers.

b. (U) DCID 1/20 Revision. This revision also primarily reflects format and editorial revisions. Exceptions are as follows:

(1) (U) The NSA member noted that the current DCID 1/20 provides that unofficial travel to the hazardous areas without official approval may result in the withdrawal of continued SCI access approval only for persons with specific and extensive knowledge. The members agreed that this sanction should be applied to all SCI-indoctrinated persons--not just those with extensive knowledge--and included wording to this effect in paragraph 3b.

(2) (C) The appendix was amended to provide that "any form of transportation facilities owned or controlled by an activity within a listed country" be considered a hazardous

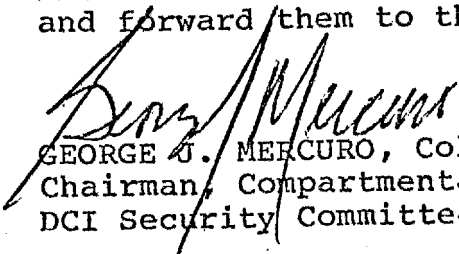
OS 2 2593

~~CONFIDENTIAL~~CLASSIFIED BY: DCID 1/20
DECLASSIFY ON: OADR

CONFIDENTIAL

activity. This was proposed by the Air Force member in view of the known hazards associated with using such facilities, e.g., traveling aboard the Soviet "Odessa" type "cruise ships."

3. (U) The Compartmentation Subcommittee recommends that the DCI SECDEF endorse the attached revisions of DCID 1/7 and DCID 1/20 and forward them to the NFIB for further consideration.


GEORGE J. MERCURO, Colonel, USAF
Chairman, Compartmentation Subcommittee
DCI Security Committee

2 Atchs

1. DCID 1/7 Revision (U)
2. DCID 1/20 Revision (C)

CONFIDENTIAL

DISSEMINATION OF INTELLIGENCE INFORMATION¹

(Effective _____ 1982)

Pursuant to the provisions of the Director of Central Intelligence Directive (DCID) on the Security Committee (SECOM), the following controls on the dissemination and use of intelligence information and related materials (hereafter referred to as intelligence)² are hereby established.

1. Purpose

These provisions establish certain common controls and procedures for the dissemination and use of intelligence to ensure that, while facilitating its interchange for intelligence purposes, it will be adequately protected. These provisions amplify applicable portions of the 23 June 1982 Information Security Oversight Office (ISOO) Directive #1 which implements Executive Order (EO) 12356. They also prescribe additional controls on the dissemination of intelligence to foreign governments and to foreign nationals and immigrant aliens, including those employed by the US Government. Policy on release of intelligence to contractors and consultants is set forth in the Appendix.

2. General

a. Applicability. The controls and procedures set forth in these provisions shall be uniformly applied in the dissemination and use of intelligence originated by all Intelligence Community organizations as defined by EO 12333.

¹ These provisions supersede DCID No. 1/7, effective 4 May 1981.

² For purposes of these provisions the terms "intelligence information and related materials" (or "intelligence") mean:

(1) "Foreign intelligence and counterintelligence," as these terms are defined in EO 12333, and

(2) Information describing US foreign intelligence and counterintelligence activities, sources and methods, equipment, and methodology used for the acquisition, processing, or exploitation of such intelligence, foreign military hardware obtained for exploitation, and photography or recordings resulting from such US intelligence collection efforts.

b. **Implementation.** The substance of these provisions shall be published in appropriate regulatory or notice media of each Intelligence Community organization, together with appropriate procedures permitting rapid interagency consultation concerning the dissemination and use of intelligence. For this purpose, each Intelligence Community organization will designate a primary referent. Originators of intelligence bearing control markings or other restrictions required by these provisions, shall ensure that requests concerning them are answered promptly.

c. **"Need-To-Know" Principle.** "Need-to-know" is a determination by an authorized holder of classified information that access to specific classified material in his or her possession is required by one or more other persons to perform a specific and officially authorized function essential to accomplish a national security task or as required by Federal Statute, Executive Order, or directly applicable regulation. In addition to an established "need-to-know," a person must possess an appropriate security clearance and access approvals, as required; prior to being provided classified information.

3. Use and Dissemination Among US Intelligence Community Organizations

a. **"Third Agency" Rule.** EO 12356 states that classified information originating in one US agency shall not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. This is commonly described as the "third agency" rule.

b. **Advance Authorization.** To facilitate the dissemination and different uses made of classified intelligence within and among Intelligence Community organizations and to assure the timely provision of intelligence to consumers, it is necessary to provide controlled relief to the "third agency rule" within the Intelligence Community in addition to that provided by the National Security Act of 1947 [50 USC 403 (d)]. Accordingly, Intelligence Community organizations are hereby authorized to use each other's classified intelligence in their respective intelligence documents, publications or other information media, and to disseminate their products to other Intelligence Community organizations except as specifically restricted by control markings prescribed in paragraph 6. Classified intelligence documents, even though they bear no control markings will not be released in their original form to third agencies without permission of the originator.

4. Use and Dissemination To Other US Organizations

Classified intelligence, even though it bears no restrictive control marking, will not be released in its original form to US organizations outside of the Intelligence Community without permission of the originator. Any organization disseminating intelligence beyond the organizations of the Intelligence Community shall be responsible for ensuring that recipient organizations understand and agree to observe the restrictions prescribed by these provisions and maintain adequate safeguards.

5. Foreign Dissemination of Intelligence

a. Dissemination to Immigrant Aliens, Foreign Contractors, and Other Foreign Nationals.

(1) Classified intelligence, even though it bears no control markings, will not be released to foreign nationals and immigrant aliens (including US Government employed, utilized or integrated foreign nationals and immigrant aliens) without permission of the originator.

(2) Release of classified intelligence to a foreign contractor/company under contract to the US Government will be made according to paragraph 5b through the government under which the contractor/company operates. Direct US-to-foreign contractor/company release is prohibited.

b. Dissemination to Foreign Governments.

Classified intelligence, even though it bears no control markings authorized by these provisions, will not be released in its original form to foreign governments without permission of the originator. Information contained in classified intelligence of another Intelligence Community organization, and which bears no restrictive control markings, may be used by the recipient Intelligence Community organization in reports disseminated to foreign governments³ provided:

(1) No reference is made to the source documents upon which the released product is based.

(2) The information is extracted or paraphrased to insure that the source or manner of acquisition of the intelligence cannot be deduced or revealed in any manner.

(3) Foreign release is made through established foreign disclosure channels and procedures, such as prescribed pursuant to the on the Committee on Imagery Requirements and Exploitation (COMIREX) and the Signals Intelligence (SIGINT) Committee.

³ Excepting RESTRICTED DATA and FORMERLY RESTRICTED DATA, which is prohibited from foreign dissemination under Sections 123 and 144 of Public Law 585, Atomic Energy Act of 1954, as amended.

6. Authorized Control Markings

a. "WARNING NOTICE--INTELLIGENCE SOURCES OR METHODS INVOLVED" (WNINTEL)

(1) This marking is used, with a security classification, to identify information whose sensitivity requires constraints on its further dissemination and use. This marking may be used only on intelligence which identifies or would reasonably permit identification of an intelligence source or method which is susceptible to countermeasures that could nullify or reduce its effectiveness.

(2) Classified intelligence so marked shall not be disseminated in any manner outside authorized channels⁴ without the permission of the originating agency and an assessment by the Senior Official of the Intelligence Community (SOIC) in the disseminating agency as to the potential risks to the national security and to the intelligence source and methods involved. In making such assessment, consideration should be given to reducing the risk to the intelligence sources or methods which provided the intelligence by sanitizing or paraphrasing the information so as to permit its wider dissemination. To avoid confusion as to the extent of dissemination and use restrictions governing the information involved, the marking may not be used in conjunction with special access or Sensitive Compartmented Information (SCI) controls. This marking may be abbreviated as "WNINTEL" or as "WN."

b. "DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR" (ORCON)

(1) This marking is used, with a security classification, to enable a continuing knowledge and supervision by the originator of the use made of the information involved. This marking may be used only on intelligence which clearly identifies or would reasonably permit ready identification of an intelligence source or method which is particularly susceptible to countermeasures that would nullify or measurably reduce its effectiveness. This marking may not be used when an item of information will reasonably be protected by use of any other markings specified herein, or by the application of the "need-to-know" principle and the safeguarding procedures of the security classification system.

⁴ Unless otherwise specified by the Director of Central Intelligence in consultation with the National Foreign Intelligence Board (NFIB) or as agreed to between originating and recipient agencies, authorized channels are the Intelligence Community, as defined in EO 12333, and Intelligence Community contractors and consultants and officials of agencies represented on the NFIB as determined on a "need-to-know" basis by recipient Senior Officials of the Intelligence Community (SOIC).

(2) Information bearing this marking may not be disseminated beyond the headquarters elements⁵ of the recipient organizations and may not be incorporated in all or in part into other reports or briefings without the advance permission of and under conditions specified by the originator. As this is the most restrictive marking herein, agencies will establish procedures to ensure that it is only applied to particularly sensitive intelligence and that timely procedures are established to review requests for further dissemination of intelligence bearing this marking. This marking may be abbreviated as "ORCON" or as "OC."

c. "NOT RELEASABLE TO CONTRACTORS/CONSULTANTS" (NOCONTRACT)

This marking is used, with a security classification, to prohibit the dissemination of information to contractors or consultants (hereinafter contractors) without the permission of the originating agency. This marking may be used only on intelligence which, if disclosed to a contractor, would actually or potentially give him a competitive advantage which could reasonably be expected to cause a conflict of interest with his obligation to maintain the security of the information; or which was provided by a source on the express or implied condition that it not be made available to contractors. The restrictions applicable to this marking do not apply to consultants hired under Office of Personnel Management procedures, or comparable procedures derived from authorities vested in heads of organizations by law, and who are normally considered to be extensions of the office by which they are employed. This marking may be abbreviated as "NOCONTRACT" or as "NC."

d. "CAUTION--PROPRIETARY INFORMATION INVOLVED" (PROPIN)

This marking may be used, with or without a security classification, to identify information provided by a commercial firm or private source under an express or implied understanding that the information will be protected as a trade secret or proprietary data believed to have actual or potential value. Information bearing this marking shall not be disseminated in any form to an individual, organization, or foreign government which has any interests, actual or potential, in competition with the source of the information without permission of the originator. This marking may be used in conjunction with the "NOCONTRACT" marking to preclude dissemination to any contractor. This marking may be abbreviated as "PROPIN" or as "PR."

⁵ At the discretion of the originator, the term "headquarters elements" may include specified subordinate intelligence-producing components.

e. "NOT RELEASABLE TO FOREIGN NATIONALS" (NOFORN)

This marking is used with a security classification to identify intelligence that may not be released in any form to foreign governments, foreign nationals, or non-US citizens without permission of the originator. This marking may be used on intelligence which if released to a foreign government or national(s) could jeopardize intelligence sources or methods, or when it would not be in the best interests of the US to release the information from a policy standpoint upon specific determination by a Senior Official of the Intelligence Community (SOIC). SOICs are responsible for developing, publishing and maintaining guidelines consistent with the policy guidance herein for use in determining the foreign releasability of intelligence they collect or produce. These guidelines shall be used in assigning NOFORN control markings, and by primary referents (paragraph 2b above applies) in responding to inquiries from other organizations on application of this control. This marking may be abbreviated "NOFORN" or as "NF."

f. "AUTHORIZED FOR RELEASE TO (name of country(ies)/international organization)" (REL _____)

This marking is used to identify classified intelligence that an originator has predetermined to be releasable or has released, through established foreign disclosure procedures and channels, to the foreign country(ies)/organization indicated. No other foreign dissemination of the material is authorized (in any form) without the prior approval of the originator. This marking may be abbreviated "REL (abbreviated name of country(ies)/international organization)." In the case of intelligence and related material controlled under DCID 6/2, authorized distribution indicators, published separately, may be used instead of the "REL" control marking.

7. Procedures Governing Use of Control Markings

a. Any recipient desiring to use intelligence in a manner contrary to the restrictions established by the control markings set forth above shall obtain the advance permission of the originating agency. Such permission applies only to the specific purpose agreed to by the originator and does not automatically apply to all recipients. Originators should insure that prompt consideration is given to recipients' requests in these regards, with particular attention to reviewing, and editing if necessary, sanitized or paraphrased versions to derive a text suitable for release subject to lesser or no control markings.

b. The control markings authorized above shall be shown on the title page, front cover, and other applicable pages of documents, incorporated in the text of electrical communications, shown on graphics, and associated (in full or abbreviated form)

with data stored or processed in automatic data processing systems. The control markings also shall be indicated by parenthetical use of the marking abbreviations at the beginning or end of the appropriate portions. If the control markings apply to several or all portions, the document may be marked with a statement to this effect rather than marking each portion individually.

c. The control markings in paragraph 6 shall be individually assigned at the time of preparation of intelligence products and used in conjunction with security classifications and other markings specified by EO 12356 and its implementing ISOO Directive. The markings shall be carried forward to any new format in which the same information is incorporated, including oral and visual presentations.

8. Reporting Unauthorized Disclosures

Violations of the foregoing restrictions and control markings that result in unauthorized disclosure by one agency of the intelligence of another shall be reported to the Director of Central Intelligence through the DCI Security Committee.

9. Obsolete Restrictions and Markings

The following markings are obsolete and will not be used subsequent to the date of these procedures: WARNING NOTICE-SENSITIVE SOURCES AND METHODS INVOLVED, WARNING NOTICE-INTELLIGENCE SOURCES AND METHODS INVOLVED, CONTROLLED DISSEM, NSC PARTICIPATING AGENCIES ONLY, INTEL COMPONENTS ONLY, LIMITED, CONTINUED CONTROL, NO DISSEM ABROAD, BACKGROUND USE ONLY, WARNING NOTICE-SENSITIVE INTELLIGENCE SOURCES AND METHODS INVOLVED, NO FOREIGN DISSEM, USIB ONLY, and NFIB ONLY. Questions with respect to the current application of control markings authorized by earlier directives on the dissemination and control of intelligence and used on documents issued prior to the date of these procedures should be referred to the originating agency or department.

Appendix

DCI Policy on Release of Intelligence Information
to Contractors and Consultants

APPENDIX

DCI POLICY ON RELEASE OF INTELLIGENCE
INFORMATION TO CONTRACTORS AND CONSULTANTS¹

1. So that Intelligence Community agencies may better discharge their responsibilities, they may release selected intelligence information and related materials (hereafter referred to as intelligence)² to contractors and consultants (hereafter referred to as contractors) without referral to the originating agency, provided that:

¹ General policy is set forth in "Security Control on the Dissemination of Intelligence Information," effective _____ 1982. In accordance with paragraph 6c therein, Intelligence Community organizations agree that government-owned, contractor-operated (GOCO) laboratories performing classified services in support of the intelligence mission of an Intelligence Community organization, and which are designated authorized channels by the Senior Official of the Intelligence Community (SOIC) (as defined in Executive Order (EO) 12333) (or their designated representatives) concerned, are not considered contractors for the purposes of this policy statement. See "Security Policy for Sensitive Compartmented Information (SCI)," effective 28 June 1982, for minimum standards for control of SCI released to contractors.

² For purposes of this appendix, the terms "selected intelligence information and related materials" (or "intelligence") mean:

(1) "Foreign intelligence" and "counterintelligence" as these terms are defined in EO 12333.

(2) Information describing US foreign intelligence and counterintelligence activities sources and methods, equipment and methodology used for the acquisition, processing, or exploitation of such intelligence, foreign military hardware obtained for exploitation, and photography or recordings resulting from such US intelligence collection efforts.

(3) Intelligence produced and disseminated by CIA, INR/State, DIA, NSA, ACSI/Army, ACSI/Air Force, Naval Intelligence Command, DOE and the military commands. This specifically excludes Foreign Service reporting and SCI. Permission to release Foreign Service reporting must be obtained from the Department of State. Release of SCI is governed by lateral agreements and advisements between Intelligence Community organizations.

a. Release³ is made only to private individuals or organizations certified by the Senior Official of the Intelligence Community (SOIC) (as defined in EO 12333) (or his/her designated representative) of the sponsoring organization as being under contract to the United States Government for the purpose of performing classified services in support of the mission of his/her or a member organization⁴; as having a demonstrated "need-to-know;" and an appropriate security clearance or access approval. If retention of intelligence by the contractor is required, the contractor must have an approved storage facility.

b. The SOIC of the sponsoring agency, or his/her designee(s), is responsible for ensuring that releases to contractors are made pursuant to this policy statement and through established channels.

c. The sponsoring agency maintains a record of material released.

d. Contractors maintain such records as will permit them to account for all intelligence received, disposed of or destroyed, produced and held by them for the duration of the contract, and to permit identification of all persons who have had access to intelligence in their custody.

e. Contractors do not reproduce any intelligence without the permission of the sponsoring agency, and classify, control and account for reproduced copies in the same manner as for originals.

f. Contractors destroy intelligence only according to guidelines and by standards set by the sponsoring agency.

g. Contractors make provisions to ensure that intelligence in their custody is not released to foreign nationals, whether or not they are employees or contractors themselves, except with the permission of the originating agency through the sponsoring agency.

³ Release is the authorized visual, oral, or physical disclosure of classified intelligence.

⁴ Non-Intelligence Community government components under contract to fulfill an intelligence support role, may be treated as members of the Intelligence Community rather than as contractors. When so treated, it shall be solely for the specific purposes agreed upon and shall in no case include authority to disseminate further intelligence made available to them.

h. Contractors receiving intelligence do not release it: (1) to any of their components or employees not directly engaged in providing services under the contract; or (2) to any other contractor (including subcontractors), without the consent of the sponsoring agency (which shall verify that any second contractors satisfy all security requirements herein).

i. Contractors agree that all intelligence released to them, all reproductions thereof, and all other material they may generate based on or incorporating data therefrom (including authorized reproductions), remain the property of the US Government and will be returned upon request of the sponsoring agency or expiration of the contract, whichever comes first.

j. Sponsoring agencies arrange for and contractors agree that, upon expiration of contracts, (1) all released intelligence, all reproductions thereof, and all other materials based on or incorporating data therefrom, are returned to the sponsoring agency; or (2) all or a specified part of such items are retained by the contractor under all applicable security and accountability controls when the contractors have a specific need for such retention that are validated by sponsoring agencies.

k. Sponsoring agencies delete: (1) the CIA seal, (2) the phrase "Directorate of Operations," (3) the place acquired, (4) the field number, (5) the source description, and (6) field dissemination, from all CIA Directorate of Operations reports passed to contractors, unless prior approval to do otherwise is obtained from CIA.

2. National Intelligence Estimates (NIEs), Special National Intelligence Estimates (SNIEs), National Intelligence Analytical Memoranda and Interagency Intelligence Memoranda may not be released to contractors. Such materials shall be marked NOT RELEASABLE TO CONTRACTORS/CONSULTANTS. However, information in them may be made available to contractors, without identification as national intelligence by the SOIC of the agency authorizing its release.

3. Intelligence which by reason of sensitivity of content bears control markings "CAUTION--PROPRIETARY INFORMATION INVOLVED," "NOT RELEASABLE TO CONTRACTORS/CONSULTANTS," or "DISSEMINATION AND EXTRACTION OF INFORMATION CONTROLLED BY ORIGINATOR," as contained in DCID, "Control of Dissemination of Intelligence Information," may not be released to contractors unless special permission has been obtained from the originator.

4. The contracting with private sector firms for operation of Intelligence Community all-source telecommunications centers (or similar activities) presents serious concerns regarding necessary

security protection for the wide range of sensitive intelligence flowing into such centers. It is DCI policy that use of contractors to operate an all-source telecommunications center in an Intelligence Community activity would necessitate exploring other channels (such as couriers) for delivery of intelligence information. While this would result in regrettable time delays, security requirements dictate that the Community not expose an unnecessarily wide range of intelligence information to contractor personnel.

5. Questions concerning the implementation of this policy and these procedures shall be referred for appropriate action to the DCI Security Committee.

~~CONFIDENTIAL~~

SECURITY POLICY CONCERNING TRAVEL AND ASSIGNMENT OF
PERSONNEL WITH ACCESS TO SENSITIVE COMPARTMENTED
INFORMATION (SCI)¹

(Effective _____ 1982)

Pursuant to the provisions of the Director of Central Intelligence Directive (DCID) on the Security Committee, minimum security policy is herewith established for assignment and travel of U.S. Government civilian and military personnel, government consultants and employees of government contractors who have, or who have had, access to SCI.

1. Purpose

This policy is based upon the need to protect SCI from possible compromise resulting from the capture, interrogation, exploitation, or entrapment of personnel (stipulated above) by hostile nations or groups.

2. Definitions

a. Defensive Security Briefings--formal advisories which alert traveling personnel to the potential for harassment, provocation, or entrapment. These briefings are based on actual experience when available, and include information on courses of action helpful in mitigating adverse security and personal consequences.

b. Hazardous Activities--include assignments or visits to, and travel through, countries listed in the attached Appendix. Hazardous activities also include assignment or travel in combat zones or other areas where hostilities are taking place, duties behind hostile lines, and duties or travel in isolated or exposed areas where individuals cannot reasonably be protected against hostile action.

c. Risk of Capture Briefings--formal advisories which alert personnel as to what may be expected in the way of attempts to force or trick them to divulge classified information if captured or detained and of suggested courses of action they should follow to avoid or limit such divulgence. These advisories include instructions/advice for advance preparation of innocuous, alternate explanations of duties and background.

¹ This policy statement supersedes DCID No. 1/20, effective 6 June 1978.

CLASSIFIED BY: _____
DECLASSIFY ON: _____ OADR

~~CONFIDENTIAL~~

CONFIDENTIAL

d. Senior Officials of the Intelligence Community (SOIC)--for the purposes of this policy statement, SOICs are defined as the heads of organizations within the Intelligence Community, as defined by Executive Order 12333, or their designated representatives.

e. Sensitive Compartmented Information (SCI)--all information and materials requiring special community controls indicating restricted handling within present and future community intelligence collection programs and their end products. These special Community controls are formal systems of restricted access established to protect the sensitive aspects of sources, methods and analytical procedures of foreign intelligence programs. The term does not include Restricted Data as defined in Section II, Public Law 585, Atomic Energy Act of 1954, as amended.

3. Policy

a. Unofficial Travel. Persons granted authorization for access to certain categories of extremely sensitive information on foreign intelligence sources or methods of SCI incur a special security obligation and are to be alerted by their SOIC to risks associated with unofficial visits to, or travel through, the countries listed in the Appendix hereto. The SOIC concerned should advise that unofficial travel in the listed countries without official approval may result in the withdrawal of approval for continued access to SCI for persons with specific and extensive knowledge of the following categories of extremely sensitive information on foreign intelligence sources or methods:

- Technological structure, function, and techniques of sensitive intelligence collection or exploitation system/methods.
- Designated system targets or sources.
- Method and purpose of target selection.
- Degree of success of collection or exploitation system/method.
- Collection or exploitation system/method capabilities and vulnerabilities.

b. All persons having access to SCI who plan unofficial travel to or through countries listed in the Appendix hereto must:

- (1) Give advance notice of such planned travel.

CONFIDENTIAL

CONFIDENTIAL

(2) Obtain a defensive security briefing from a specified official before traveling to such countries.

(3) Contact immediately the nearest U.S. consular, attache, or Embassy official if they are detained or subjected to significant harassment or provocation while traveling.

(4) Report upon return from travel to their SOIC any incidents of potential security concern which befell them.

(5) Be reminded annually of the foregoing obligations through security education programs.

Failure to comply with the provisions of (1) and (4) above may be cause for withdrawal of SCI access authorization.

c. Official Assignment/Travel. No person with access to SCI will be assigned to or directed to participate in hazardous activities until he or she has been afforded a defensive security briefing and/or risk of capture briefing as applicable. (Due consideration will be given to the relative protection enjoyed by U.S. officials having diplomatic status.)

d. Individuals with Previous SCI Access. Persons whose access to SCI is being terminated will be officially reminded of the risks associated with hazardous activities as defined herein and of their obligation to ensure continued protection of SCI.

4. Responsibilities

a. The DCI will cause to be prepared and disseminated to the SOICs a list of countries identified as posing a security risk bearing on this policy (see Appendix). The Security Committee will coordinate required support including source material concerning these risks.

b. SOICs will issue implementing directives concerning travel and assignment of personnel of their departments or agencies. Such directives will include the overall policy, definitions, and criteria set forth herein and will provide for:

(1) Preparation and provision of defensive security briefings or risk of capture briefings to personnel of their departments or agencies.

(2) Institution of positive programs for the collection of information reported under the provisions of paragraph 3b(4), above

(3) Ensuring that new information obtained by their departments or agencies on harassments or provocations, or on risk

CONFIDENTIAL

~~CONFIDENTIAL~~

of capture situations, is provided to the DCI and to other interested NFIB agencies. (Where warranted by new information, changes to the Appendix hereto will be made. Recommendations with supporting justification may be made for either addition or deletion of countries.)

5. Classification. As this directive sets forth security policy for persons with access to SCI, it merits and warrants the overall classification of CONFIDENTIAL in its totality. Selected paragraphs may be excerpted for use at the FOR OFFICIAL USE ONLY level by SOICs, their designees, or SCI Special Security/Control Officers, when considered appropriate.

Appendix:

Countries and Areas in Which Visits, Travel, and Assignment are Considered to be a Hazardous Activity

~~CONFIDENTIAL~~

Page Denied

ROUTING AND RECORD SHEET				
SUBJECT: (Optional) Revision of DCIDs 1/7 and 1/20				
FROM: [redacted] DC/Physical Security Division		EXTENSION	NO.	
			DATE 5 November 1982	
TO: (Officer designation, room number, and building)	DATE RECEIVED FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)	
1. C/PSD				
2. C/OPS/PTAS	NOV 10-8 1982		<i>Concurrence - renew comments -</i>	
3. DD/PTAS	11-8-82			
4. C/OS/PPG 4E70 Hqs	11/8/82	Seen	<p>5 to 4: Upon receipt today of the attached comments from DC/PSD/OS. I checked back with [redacted] SSC. He noted that the System has been working for years, and that the only substantive revision being accomplished here is a change in the numbers of the Executive Order(s), from 12065 to 12356. Bob does not feel that the PSD-suggested changes are substantive enough to have [redacted] raise them before SECDEF. I believe we should accept Bob's counsel, and am documenting the record as to why.</p> <p>4-5: Before going forward, check back with [redacted] 15/8</p> <p>5: I discussed above with [redacted] on 11/9/82. He did not feel so strongly about his comments that they need to go forward to SECDEF. Hence, PPG will recommend that D/S [redacted] concur with the drafts as presented.</p>	
5. [redacted] OS/PPG	11/9/82	20		
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.		from		
15.				